Amendments to the Claims

Please cancel Claims 8, 9, 21, and 22. Please amend Claims 1, 4, 5, 10, 13, 17, and 18. The Claim Listing below will replace all prior versions of the claims in the application:

Claim Listing

1. (Currently amended) A system for providing a usage accountability model for data security in a data processing ~~system~~ system, comprising:

a user client device having (i) a sensor to sense atomic level events at a point of authorized access to at least one digital asset by an end user of the user client device, the sensor located within an operating system kernel within the user client device, (ii) a filter to filter the atomic level events with an approved event list, the filter filtering out atomic level events not corresponding to approved events, and (iii) a coalescing aggregator to aggregate sets of atomic level events relating to respective single end user actions into single atomic level events, resulting in coalesced atomic level events, and to bundle and encrypt the coalesced atomic level events, resulting in bundles of coalesced atomic level events; and

a journaling server having [[an]] a high-level aggregator (i) to accept the bundles of coalesced atomic level events from the user client device, (ii) to decrypt the bundles of coalesced atomic level events, (iii) to store the coalesced atomic level events in a table having fields relating to the coalesced atomic level events including event type, event category, event name, event detail, and event discriminant, and (iv) to aggregate at least some of the coalesced atomic level events to generate at least one aggregate event based on at least one predetermined sequence of atomic level events, and having a reporter to generate an audit trail from the at least one aggregate event, the audit trail representing usage of the at least one digital asset by the end user.

2. (Previously presented) A system as in claim 1 wherein the aggregate events are associated with a particular executing process.

3. (Previously presented) A system as in claim 2 wherein the executing process is associated with the end user.

4. (Currently amended) A system as in claim 1 ~~wherein the user client device further includes a filter for filtering the atomic level events with an approved event list, and~~ wherein the high-level aggregator only accepts atomic level events not filtered out by the filter.

5. (Currently amended) A system as in ~~claim 4~~ claim 1 wherein the approved event list includes a list of approved file identifiers.

6. (Previously presented) A system as in claim 5 wherein the file identifiers are a hash code.

7-9. (Canceled)

10. (Currently amended) A system as in ~~claim 9~~ claim 1 wherein sequence numbers are added to the bundles.

11. (Previously presented) A system as in claim 1 wherein the at least one aggregate event is detected as a suspect action with a data file.

12. (Previously presented) A system as in claim 1 wherein the at least one aggregate event is attributable to the end user, a thread and/or an application as identified at a known time.

13. (Currently amended) A system as in ~~claim 8~~ claim 1 wherein the ~~coalescer~~ coalescing aggregator reports a single coalesced event after a time out period with no activity.

14. (Previously presented) A system as in claim 1 wherein the at least one aggregate event and the audit trail are used to control security of the data processing system by

determining patterns of unexpected behavior based on the at least one aggregate event and the audit trail.

15. (Previously presented) A system as in claim 1 wherein the aggregate events and the audit trail provide a perimeter of accountability for usage of the at least one digital asset at a point of use of the at least one digital asset.

16. (Previously presented) A system as in claim 15 wherein the point of use is the user client device and the accountability is of access, modification, and distribution of the at least one digital asset.

17. (Currently amended) A method for providing a usage accountability model for data security in a data processing ~~system~~ system, the method comprising:

sensing atomic level events at a point of authorized access to at least one digital asset by an end user of a user client device of the data processing system, the sensing taking place in an operating system kernel within the user client device;

filtering out atomic level events not corresponding to approved events using an approved event list;

aggregating sets of atomic level events relating to respective single end user actions into single atomic level events, resulting in coalesced atomic level events;

bundling and encrypting the coalesced atomic level events, resulting in bundles of coalesced atomic level events;

forwarding the bundles of coalesced atomic level events to a journaling server of the data processing system;

decrypting the bundles of coalesced atomic level events;

storing the coalesced atomic level events in a table having fields relating to the coalesced atomic level events including event type, event category, event name, event detail, and event discriminant;

aggregating at least some of the coalesced atomic level events at the journaling server to generate at least one aggregate event based on at least one predetermined sequence of atomic level events; and

generating an audit trail from the at least one aggregate event, the audit trail representing usage of the at least one digital asset by the end user.

18. (Currently amended) A method as in claim 17 ~~further including filtering the atomic level events with an approved event list, and~~ wherein forwarding the bundles of coalesced atomic level events to the journaling server includes forwarding only atomic level events not filtered out by the approved event list.

19. (Original) A method as in claim 18 where the approved event list includes a list of approved file identifiers.

20-22. (Canceled)

23. (Previously presented) A system as in claim 1 wherein the usage of the at least one digital asset includes access and dissemination of the at least one digital asset.

24. (Previously presented) A method as in claim 17 wherein the usage of the at least one digital asset includes access and dissemination of the at least one digital asset.